Courtney E. Maccarone (NJ 029842011)
LEVI & KORSINSKY, LLP
33 Whitehall Street, 17th Floor
New York, NY 10004
Telephone: (212) 363-7500
Facsimile: (212) 363-7171
Email: cmaccarone@zlk.com

[*Additional Counsel listed on signature page*]

Counsel for Plaintiffs

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW JERSEY

MINDY MARKOWITZ and BRENDA LITTLE, individually and on behalf of all others similarly situated, Plaintiffs, v. HealthEC, LLC Defendant.	**CASE NO.: 2:24-cv-172** **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiffs Mindy Markowitz and Brenda Little, individually and on behalf of all others similarly situated, by and through their undersigned counsel, bring this Class Action Complaint against HealthEC LLC (herein "HEC" or "Defendant"). Plaintiffs allege the following upon information and belief based on the investigation of counsel, except as to those allegations that specifically pertain to Plaintiffs, which are alleged upon personal knowledge.

INTRODUCTION

1. Plaintiffs and the proposed Class Members bring this class action lawsuit on behalf of all persons who entrusted HEC with personally identifiable information ("PII"),[1] protected health information ("PHI") and billing and claims information ("Private Information") that was subsequently exposed in a data breach, which HEC publicly disclosed on December 22, 2023 (the "Data Breach" or the "Breach").[2]

2. Plaintiffs' claims arise from Defendant's failure to properly secure and safeguard PII, PHI, and Private Information that was entrusted to it, and the accompanying responsibility to store and transfer that information. Over 4.5 million patients' information was affected by the Data Breach, including names, Social Security numbers, medical record numbers, billing information, and claims information.[3]

3. HEC, based in Edison, New Jersey, is an analytics software vendor, which helps develop and deliver end-to-end technology solutions for exchanging healthcare information and managing population health technology company.[4]

4. On or around July 14 and July 23, 2023, a successful attack on Defendant's information technology network occurred.[5] Upon becoming aware of the suspicious activity, HEC launched an investigation that included (i) confirming the security of the network, (ii) reviewing the relevant files and systems, (ii) taking actions to remediate the systems and mitigate

---

[1] Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual.

[2] *Data Breach Notifications: HealthEC, LLC*, OFFICE OF THE MAINE ATTORNEY GENERAL https://apps.web.maine.gov/online/aeviewer/ME/40/4680936e-e496-43ed-a35d-59ece9b523b6.shtml (last visited January 8, 2024).

[3] *Id.*

[4] HEALTHEC, https://www.healthec.com/ (last visited January 8, 2023).

[5] *Data Breach Notifications: HealthEC, LLC*, OFFICE OF THE MAINE ATTORNEY GENERAL https://apps.web.maine.gov/online/aeviewer/ME/40/4680936e-e496-43ed-a35d-59ece9b523b6.shtml (last visited January 8, 2024).

potential risk to data, and (iv) notifying potentially affected clients, individuals, and (v) notified federal law enforcement regarding the event and cooperated with their investigation. [6]

5. On October 24, 2023, Defendant learned that the Data Breach impacted several of the following PII, PHI and Private Information:

a. Name, address, date of birth

b. Social Security or Taxpayer Identification number

c. Medical Record number

d. Medical information (including but not limited to Diagnosis, Diagnosis Code, Mental/Physical Condition, Prescription information, and provider's name and location)

e. Health insurance information (including but not limited to beneficiary number, subscriber number, Medicaid/Medicare identification)

f. Billing and Claims information (including but not limited to patient account number, patient identification number, and treatment cost information).[7]

6. Furthermore, Defendant's investigation concluded that patients from the following healthcare services providers and state-level health systems clients of HealthEC were impacted by the cyberattack on the HealthEC tech solutions provider:

a. Advantage Care Diagnostic & Treatment Center, Inc.,

b. Alliance for Integrated Care of New York, LLC,

c. Beaumont ACO,

d. Community Health Care Systems,

e. Compassion Health Care,

f. Corewell Health,

g. East Georgia Healthcare Center,

h. HonorHealth,

[6] *Id.*
[7] *Id.*

i. Hudson Valley Regional Community Health Centers,

j. Illinois Health Practice Alliance, LLC,

k. KidneyLink,

l. Long Island Select Healthcare,

m. Metro Community Health Centers,

n. Mid Florida Hematology & Oncology Centers, P.A, d/b/a Mid-Florida Cancer Centers,

o. TennCare,

p. University Medical Center of Princeton Physicians' Organization, and

q. Upstate Family Health Center, Inc.[8]

7. Defendant had numerous statutory, regulatory, contractual, and common law duties and obligations, including those based on their affirmative representations to Plaintiffs and the Class, to keep their PII, PHI and Private Information confidential, safe, secure, and protected from unauthorized disclosure or access.

8. Plaintiffs' claims arise from Defendant's failure to safeguard PII, PHI and Private Information provided by and belonging to their customers and failure to provide timely notice of the Data Breach.

9. Defendant failed to take precautions designed to keep their customers' PII, PHI, and Private Information secure.

10. Defendant owed Plaintiffs and Class Members a duty to take all reasonable and necessary measures to keep the PII, PHI and Private Information they collected safe and secure from unauthorized access. Defendant solicited, collected, used, and derived a benefit from the PII, PHI and Private Information, yet breached their duty by failing to implement or maintain adequate security practices.

[8] *Id.*

11. Defendant admits that information in their system was accessed by unauthorized individuals, though they have provided little information on how the data breach occurred.

12. The sensitive nature of the data exposed through the Data Breach, including Social Security numbers, medical records, claims history and health data signifies that Plaintiffs and Class members have suffered irreparable harm. Plaintiffs and Class members have lost the ability to control their private information and are subject to an increased risk of identity theft.

13. Defendant also inexcusably delayed disclosing and providing notice of the Data Breach to their customers. Defendant believes that the Data Breach occurred on or around July 14 and July 23, 2023. Despite Defendant's public disclosure on October 26, 2023 regarding the Data Breach, Plaintiffs were not notified until December 22, 2023.[9]

14. Defendant, despite having the financial wherewithal and personnel necessary to prevent the Data Breach, nevertheless failed to use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information it maintained for Plaintiffs and members of the Class, causing the exposure of PII, PHI, and Private Information for Plaintiffs and members of the Class.

15. As a result of Defendant's inadequate digital security and notice process, Plaintiffs' and Class members' PII, PHI, and Private Information were exposed to criminals. Plaintiffs and the Class have suffered and will continue to suffer injuries including: financial losses caused by misuse of PII, PHI, and Private Information; the loss or diminished value of their PII, PHI, and Private Information as a result of the Data Breach; lost time associated with detecting and preventing identity theft; and theft of personal and financial information.

16. Plaintiffs bring this action on behalf of all persons whose PII, PHI, and Private Information were compromised as a result of Defendant's failure to: (i) adequately protect the

[9] *Id.*

PII, PHI, and Private Information of Plaintiffs and members of the Class; (ii) warn Plaintiffs and members of the Class of Defendant's inadequate information security practices; (iii) effectively secure hardware containing protected PII, PHI, and Private Information using reasonable and adequate security procedures free of vulnerabilities and incidents; and (iv) timely notify Plaintiffs and members of the Class of the Data Breach. Defendant's conduct amounts at least to negligence and violates federal and state statutes.

17. Plaintiffs bring this action individually and on behalf of a Nationwide Class of similarly situated individuals against Defendant for: negligence; breach of implied contract; and unjust enrichment.

18. Plaintiffs seek to remedy these harms and prevent any future data compromise on behalf of themselves and all similarly situated persons whose personal data was compromised and stolen as a result of the Data Breach and who remain at risk due to Defendant's inadequate data security practices.

JURISDICTION AND VENUE

19. This Court has jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. At least one member of the Class defined below is a citizen of a different state than Defendant, and there are more than 100 putative Class members.

20. This Court has personal jurisdiction over Defendant because Defendant maintains and operates its headquarters in this District.

21. Venue is proper in these District under 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to the claims occurred in this District.

PARTIES

22. Plaintiff Mindy Markowitz is a citizen of Michigan and resides in Southfield Michigan. Plaintiff Markowitz received a notice of data breach letter – dated December 22, 2023 – from HealthEC informing her that PII and PHI were compromised in the Data Breach. As a consequence of the Data Breach, Ms. Markowitz has been forced to and will continue to invest significant time monitoring her accounts to detect and reduce the consequences of likely identity fraud. Plaintiff Markowitz is subject to substantial and imminent risk of future harm.

23. Plaintiff Brenda Little is a citizen of Michigan and resides in Wayne, Michigan. Plaintiff Little, received a notice of data breach letter – dated December 22, 2023 – from HealthEC informing her that PII and PHI were compromised in the Data Breach. As a consequence of the Data Breach, Ms. Little has been forced to and will continue to invest significant time monitoring her accounts to detect and reduce the consequences of likely identity fraud. Plaintiff Little is subject to substantial and imminent risk of future harm.

24. Defendant HealthEC, LLC is a limited liability company formed under the state laws of Delaware, with their principal place of business located in Edison, New Jersey. Defendant is an analytics software vendor, that helps develop and deliver end-to-end technology solutions for exchanging healthcare information and managing population health technology company.[10]

25. Defendant collected and continues to collect the PII, PHI and Private Information of patients throughout their usual course of business operations. By obtaining, collecting, using, and deriving benefit from Plaintiffs' and Class's PII, PHI, and Private Information, Defendant assumed legal and equitable duties to those persons, and knew or should have known that it was responsible for protecting Plaintiffs' and Class's PII, PHI, and Private Information from unauthorized disclosure and/or criminal cyber activity.

[10] HEALTHEC https://www.healthec.com/ (last visited January 8, 2023).

FACTUAL BACKGROUND

A. Background on Defendant

26. Defendant HealthEC is an analytics software vendor, that helps develop and deliver end-to-end technology solutions for exchanging healthcare information and managing population health technology company.

27. In the ordinary course of their business practices, Defendant stores, maintains, and uses an individuals' PII, PHI, and Private Information including but not limited to information such as: full names; Social Security numbers; medical record numbers, medical history, billing, and claims information.

28. Upon information and belief, Defendant made promises and representations to its patients, including Plaintiffs and Class members, that the PII, PHI, and Private Information collected from them would be kept safe, confidential, that the privacy of that information would be maintained, and that Defendant would delete any sensitive information after it was no longer required to maintain it.

29. Plaintiffs and Class members had a reasonable expectation that Defendant would keep their information confidential and secure from unauthorized access.

30. As a result of collecting and storing the PII, PHI, and Private Information of Plaintiffs and members of the Class for their own financial benefit, Defendant had a continuous duty to adopt and employ reasonable measures to protect Plaintiffs and the Class Members' PII, PHI, and Private Information from disclosure to third parties.

B. The Data Breach

31. On or around July 14 and July 23, 2023, Defendant had its internal data servers breached by unauthorized third-party hackers, which compromised highly sensitive PII, PHI, and

Private Information of more than 4.5 million patients – including, *inter alia*, their names, Social Security Numbers, medical records, and claims information.[11]

32. On December 22, 2023, HealthEC filed a public notice of Data Breach with the Attorney General of Maine disclosing that an unauthorized party had accessed their internal systems.[12] The notice reads:

> **What Happened?**
>
> HealthEC became aware of suspicious activity potentially involving our network and promptly began an investigation. The investigation determined that certain systems were accessed by an unknown actor between July 14, 2023, and July 23, 2023, and during this time certain files were copied. We then undertook a thorough review of the files in order to identify what specific information was present in the files and to whom it relates. This review identified information relating to some of our clients. We began notifying our clients on October 26, 2023, and we worked with them to notify potentially impacted individuals, including you.
>
> **What Information Was Involved?**
>
> Your name and Name, Address, Date of Birth, Social Security Number, Medical Record, Medical Information (such as Diagnosis, Diagnosis Code, Mental/Physical Condition, Prescription information, and provider's name), Health insurance information (such as beneficiary number, subscriber number, Medicaid/Medicare identification, and/or Billing and Claims information (such as patient account number, patient identification number, and treatment cost information) were present on the impacted files.

33. While Defendant sought to minimize the damage caused by the breach, it cannot and has not denied that there was unauthorized access to the PII, PHI, and Private Information of Plaintiffs and Class Members.

34. Individuals affected by the Data Breach are, and remain, at risk that their data will be sold or listed on the dark web and, ultimately, illegally used in the future.

---

[11] *Data Breach Notifications: HealthEC, LLC*, OFFICE OF THE MAINE ATTORNEY GENERAL https://apps.web.maine.gov/online/aeviewer/ME/40/4680936e-e496-43ed-a35d-59ece9b523b6.shtml (last visited January 8, 2024).

[12] *Id.*

C. Defendant's Failure to Prevent, Identify and Timely Report the Data Breach.

35. Defendant admits that unauthorized third persons accessed from their network systems sensitive information about their current and former customers.

36. Defendant failed to take adequate measures to protect its computer systems against unauthorized access.

37. Defendant was not only aware of the importance of protecting the PHI, PII, and Private Information that it maintains, as alleged, it promoted their capability to do so, as evident from HealthEC's Privacy Policy.[13] The PII, PHI, and Private Information that Defendant allowed to be exposed in the Data Breach is the type of private information that Defendant knew or should have known would be the target of cyberattacks.

38. Despite its own knowledge of the inherent risks of cyberattacks, and notwithstanding the FTC's data security principles and practices,[14] Defendant failed to disclose that its systems and security practices were inadequate to reasonably safeguard its customers' sensitive personal information.

39. The FTC directs businesses to use an intrusion detection system to expose a breach as soon as it occurs, monitor activity for attempted hacks, and have an immediate response plan if a breach occurs.[15] Immediate notification of a Data Breach is critical so that those impacted can take measures to protects themselves.

40. Despite this guidance, Defendant delayed the notification of the Data Breach. Based on Defendant's disclosure to Maine's Attorney General's Office, the Data Breach is

[13] *Privacy Policy*, HEALTHEC https://phm.healthec.com/GNYCR0165/Privacy_Policy.aspx (last visited January 8, 2024).
[14] *Protecting Personal Information: A Guide for Business*, FEDERAL TRADE COMMISSION (Oct. 2016), https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (last visited January 8, 2024).
[15] *Id.*

believed to have occurred on or around July 14 and July 23, 2023, yet Defendant did not inform the public of the Data Breach until December 22, 2023, roughly six months after the Data Breach.

D. The Harm Caused by the Data Breach Now and Going Forward.

41. Victims of data breaches are susceptible to becoming victims of identity theft.

42. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority," 17 C.F.R. § 248.201(9), and when "identity thieves have your personal information, they can drain your bank account, run up charges on your credit cards, open new utility accounts, or get medical treatment on your health insurance."[16]

43. The type of data that was accessed and compromised here – including Social Security numbers – can be used to perpetrate fraud and identity theft. Social Security numbers are widely regarded as the most sensitive information hackers can access. Social Security numbers and dates of birth together constitute high risk data.

44. Plaintiffs and Class Members face a substantial risk of identity theft given that their Social Security numbers, addresses, and dates of birth were compromised. Once a Social Security number is stolen, it can be used to identify victims and target them in fraudulent schemes and identity theft.

45. Stolen PII and PHI are often trafficked on the "dark web," a heavily encrypted part of the Internet that is not accessible via traditional search engines. Law enforcement has difficulty policing the "dark web" due to this encryption, which allows users and criminals to conceal identities and online activity.

[16] *Prevention and Preparedness*, NEW YORK STATE POLICE, https://troopers.ny.gov/prevention-and-preparedness (last visited January 8, 2024).

46. When malicious actors infiltrate companies and copy and exfiltrate the PII and PHI that those companies store, that stolen information often ends up on the dark web because the malicious actors buy and sell that information for profit.[17]

47. For example, when the U.S. Department of Justice announced its seizure of AlphaBay in 2017, AlphaBay had more than 350,000 listings, many of which concerned stolen or fraudulent documents that could be used to assume another person's identity. Other marketplaces, similar to the now-defunct AlphaBay, "are awash with [PII] belonging to victims from countries all over the world. One of the key challenges of protecting PII online is its pervasiveness. As data breaches in the news continue to show, PII about employees, customers and the public is housed in all kinds of organizations, and the increasing digital transformation of today's businesses only broadens the number of potential sources for hackers to target."[18]

48. PII and PHI remain of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[19] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[20]

49. A compromised or stolen Social Security number cannot be addressed as simply as, perhaps, a stolen credit card. An individual cannot obtain a new Social Security number without significant work. Preventive action to defend against the possibility of misuse of a Social

[17] *Shining a Light on the Dark Web with Identity Monitoring*, IDENTITYFORCE, Dec. 28, 2020, *available at:* https://www.identityforce.com/blog/shining-light-dark-web-identity-monitoring (last visited January 8, 2024).
[18] *Stolen PII & Ramifications: Identity Theft and Fraud on the Dark Web*, ARMOR, April 3, 2018, *available at:* https://res.armor.com/resources/blog/stolen-pii-ramifications-identity-theft-fraud-dark-web/ (last visited January 8, 2024).
[19] *Id.*
[20] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), available at: https://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited January 8, 2024).

Security number is not permitted; rather, an individual must show evidence of actual, ongoing fraud activity to obtain a new number. Even then, however, obtaining a new Social Security number may not suffice. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[21]

50. The PII and PHI compromised in the Data Breach demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained: "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10 times on the black market."[22]

51. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses in 2019, resulting in more than $3.5 billion in losses to individuals and business victims.[23] Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good."[24]

52. As a result of the Data Breach, the PII and PHI of Plaintiffs and Class members has been exposed to criminals for misuse. The injuries suffered by Plaintiffs and Class members, or likely to be suffered thereby as a direct result of Defendant's Data Breach, include:

a. unauthorized use of their PII and PHI;

b. theft of their personal and financial information;

c. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

---

[21] *Id.*

[22] *Experts advise compliance not same as security*, RELIAS MEDIA https://www.reliasmedia.com/articles/134827-experts-advise-compliance-not-same-as-security (last visited January 8, 2024).

[23] *2019 Internet Crime Report Released*, FBI, https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120#:~:text=IC3%20received%20467%2C361%20complaints%20in,%2Ddelivery%20scams%2C%20and%20extortion. (last visited January 8, 2024).

[24] Id.

d. damages arising from the inability to use their PII and PHI;

e. Improper disclosure of their PII and PHI;

f. loss of privacy, and embarrassment;

g. trespass and damage their personal property, including PII and PHI;

h. the imminent and certainly impending risk of having their confidential medical information used against them by spam callers and/or hackers targeting them with phishing schemes to defraud them;

i. costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach, including finding fraudulent charges, purchasing credit monitoring and identity theft protection services, and the stress, nuisance, and annoyance of dealing with all issues resulting from the Data Breach;

j. the imminent and certainly impending injury flowing from potential fraud and identify theft posed by their PII and PHI being placed in the hands of criminals and already misused via the sale of Plaintiffs' and Class members' information on the Internet black market; and

k. damages to and diminution in value of their PII entrusted to Defendant for the sole purpose of obtaining medical services from Defendant, and the loss of Plaintiffs' and Class members' privacy.

53. In addition to a remedy for economic harm, Plaintiffs and Class members maintain an interest in ensuring that their PII and PHI is secure, remains secure, and is not subject to further misappropriation and theft.

54. Defendant disregarded the rights of Plaintiffs and Class members by (i) intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that their network servers were protected against unauthorized intrusions; (ii) failing to disclose that it did not have adequately robust security protocols and training practices in place to adequately safeguard Plaintiffs' and Class members' PII and PHI; (iii) failing to take standard and reasonably available steps to prevent the Data Breach; (iv) concealing the existence

and extent of the Data Breach for an unreasonable duration of time; and (v) failing to provide Plaintiffs and Class members prompt and accurate notice of the Data Breach.

55. The actual and adverse effects to Plaintiffs and Class members, including the imminent, immediate and continuing increased risk of harm for identity theft, identity fraud and/or medical fraud directly and/or proximately caused by Defendant's wrongful actions and/or inaction and the resulting Data Breach require Plaintiffs and Class members to take affirmative acts to recover their peace of mind and personal security including, without limitation, purchasing credit reporting services, purchasing credit monitoring and/or internet monitoring services, frequently obtaining, purchasing and reviewing credit reports, bank statements, and other similar information, instituting and/or removing credit freezes and/or closing or modifying financial accounts, for which there is a financial and temporal cost. Plaintiffs and other Class members have suffered, and will continue to suffer, such damages for the foreseeable future.

CLASS ACTION ALLEGATIONS

56. Plaintiffs bring this action pursuant to Rule 23 of the Federal Rules of Civil Procedure, individually and on behalf of the following Nationwide Class:

> All persons in the United States whose personal information was compromised in the Data Breach publicly announced by Defendant in December 2023 (the "Class").

57. Specifically excluded from the Class is the Defendant their officers, directors, agents, trustees, parents, children, corporations, trusts, representatives, employees, principals, servants, partners, joint venturers, or entities controlled by Defendant, and their heirs, successors, assigns, or other persons or entities related to or affiliated with Defendant and/or its officers and/or directors, the judge assigned to this action, and any member of the judge's immediate family.

58. Plaintiffs reserve the right to amend the Class definitions above if further investigation and/or discovery reveals that the Class should be expanded, narrowed, divided into subclasses, or otherwise modified in any way.

59. This action may be certified as a class action under Federal Rule of Civil Procedure 23 because it satisfies the numerosity, commonality, typicality, adequacy, and superiority requirements therein.

60. Numerosity (Rule 23(a)(1)): The Class is so numerous that joinder of all Class members is impracticable. Although the precise number of such persons is unknown, and the facts are presently within the sole knowledge of Defendant, Plaintiffs estimate that the Class is comprised of millions of Class members. The Class is sufficiently numerous to warrant certification.

61. Typicality of Claims (Rule 23(a)(3)): Plaintiffs' claims are typical of those of other Class Members because they all had their PII compromised as a result of the Data Breach. Plaintiffs are members of the Class and their claims are typical of the claims of the members of the Class. The harm suffered by Plaintiffs is similar to that suffered by all other Class members that was caused by the same misconduct by Defendant.

62. Adequacy of Representation (Rule 23(a)(4)): Plaintiffs will fairly and adequately represent and protect the interests of the Class. Plaintiffs have no interests antagonistic to, nor in conflict with, the Class. Plaintiffs have retained competent counsel who are experienced in consumer and commercial class action litigation and who will prosecute this action vigorously.

63. Superiority (Rule 23(b)(3)): A class action is superior to other available methods for the fair and efficient adjudication of this controversy. Because the monetary damages suffered by individual Class members is relatively small, the expense and burden of individual litigation make it impossible for individual Class members to seek redress for the wrongful conduct asserted herein. If Class treatment of these claims is not available, Defendant will likely continue its wrongful conduct, will unjustly retain improperly obtained revenues, or will otherwise escape liability for its wrongdoing as asserted herein.

64. Predominant Common Questions (Rule 23(a)(2)): The claims of all Class members present common questions of law or fact, which predominate over any questions affecting only individual Class members, including:

a. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

b. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

c. Whether Defendant's storage of Class Member's PII and PHI was done in a negligent manner;

d. Whether Defendant had a duty to protect and safeguard Plaintiffs' and Class Members' PII and PHI;

e. Whether Defendant's conduct was negligent;

f. Whether Defendant's conduct violated Plaintiffs' and Class Members' privacy;

g. Whether Defendant took sufficient steps to secure their customers' PII and PHI;

h. Whether Defendant was unjustly enriched;

i. The nature of relief, including damages and equitable relief, to which Plaintiffs and members of the Class are entitled.

65. Information concerning Defendant's policies is available from Defendant's records.

66. Plaintiffs know of no difficulty which will be encountered in the management of this litigation which would preclude their maintenance as a class action.

67. The prosecution of separate actions by individual members of the Class would run the risk of inconsistent or varying adjudications and establish incompatible standards of conduct for Defendant. Prosecution as a class action will eliminate the possibility of repetitious and inefficient litigation.

68. Defendant has acted or refused to act on grounds generally applicable to the Class, thereby making appropriate final injunctive relief or corresponding declaratory relief with respect to the Class as a whole.

69. Given that Defendant has not indicated any changes to its conduct or security measures, monetary damages are insufficient and there is no complete and adequate remedy at law.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of Plaintiffs and All Class Members)

70. Plaintiffs incorporate by reference all preceding allegations, as if fully set forth herein.

71. Plaintiffs bring this claim individually and on behalf of the Class members.

72. Defendant knowingly collected, came into possession of, and maintained Plaintiffs' and Class Members' PII, PHI, and Private Information, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

73. Defendant had a duty to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiffs' and Class Members' PII, PHI, and Private Information.

74. Defendant had, and continues to have, a duty to timely disclose that Plaintiffs' and Class Members' PII, PHI, and Private Information within its possession was compromised and precisely the type(s) of information that was compromised.

75. Defendant owed a duty of care to Plaintiffs and Class Members to provide data security consistent with industry standards, applicable standards of care from statutory authority like Section 5 of the FTC Act, and other requirements discussed herein, and to ensure that their

systems and networks, and the personnel responsible for them, adequately protected their customers' PII, PHI, and Private Information.

76. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its clients. Defendant was in a position to ensure that their systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

77. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential PII, PHI, and Private Information.

78. Defendant breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class members' PII, PHI, and Private Information.

79. The specific negligent acts and omissions committed by Defendant includes, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' PII, PHI, and Private Information;

b. Failing to adequately monitor the security of their networks and systems; and

c. Failing to periodically ensure that their computer systems and networks had plans in place to maintain reasonable data security safeguards.

80. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiffs and Class members by failing to exercise reasonable care in protecting and safeguarding Plaintiffs' and Class Members' PII, PHI, and Private Information within Defendant's possession.

81. Defendant, through their actions and/or omissions, unlawfully breached their duties to Plaintiffs and Class members by failing to have appropriate procedures in place to detect and prevent dissemination of Plaintiffs' and Class Members' PII, PHI, and Private Information.

82. Defendant, through their actions and/or omissions, unlawfully breached their duty to timely disclose to Plaintiffs and Class Members that the PII, PHI, and Private Information within Defendant's possession might have been compromised and precisely the type of information compromised.

83. Defendant breached the duties set forth in 15 U.S.C. § 45, the FTC guidelines, the NIST's Framework for Improving Critical Infrastructure Cybersecurity, and other industry guidelines. In violation of 15 U.S.C. § 45, Defendant failed to implement proper data security procedures to adequately and reasonably protect Plaintiffs' and Class Member's PII, PHI, and Private Information. In violation of the FTC guidelines, inter alia, Defendant did not protect the personal customer information it keeps; failed to properly dispose of personal information that was no longer needed; failed to encrypt information stored on computer networks; lacked the requisite understanding of their networks' vulnerabilities; and failed to implement policies to correct security issues.

84. It was foreseeable that Defendant's failure to use reasonable measures to protect Plaintiffs' and Class Members' PII, PHI, and Private Information would result in injury to Plaintiffs and Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches.

85. It was foreseeable that the failure to adequately safeguard Plaintiffs' and Class Members' PII, PHI, and Private Information would result in injuries to Plaintiffs and Class Members.

86. Defendant breach of duties owed to Plaintiffs and Class Members caused Plaintiffs' and Class Members' PII, PHI and Private Information to be compromised.

87. But for Defendant's negligent conduct and breach of the above-described duties owed to Plaintiffs and Class members, their PII, PHI and Private Information would not have been compromised.

88. As a result of Defendant's failure to timely notify Plaintiffs and Class Members that their PII, PHI and Private Information had been compromised, Plaintiffs and Class Members are unable to take the necessary precautions to mitigate damages by preventing future fraud.

89. As a result of Defendant's negligence and breach of duties, Plaintiffs and Class Members are in danger of imminent harm in that their PII, PHI, and Private Information which is still in the possession of third parties, will be used for fraudulent purposes, and Plaintiffs and Class Members have and will suffer damages including: a substantial increase in the likelihood of identity theft; the compromise, publication, and theft of their personal information; loss of time and costs associated with the prevention, detection, and recovery from unauthorized use of their personal information; the continued risk to their personal information; future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the personal information compromised as a result of the Data Breach; and overpayment for the services or products that were received without adequate data security.

COUNT II
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and All Class Members)

90. Plaintiffs incorporate by reference all preceding allegations, as if fully set forth herein.

91. Plaintiffs and the Class provided and entrusted their PII, PHI, and Private Information to Defendant. Plaintiffs and the Class provided their PII, PHI and Private Information to Defendant as part of Defendant's regular business practices.

92. In so doing, Plaintiffs and the Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiffs and the Class if their data had been breached and compromised or stolen, in return for the business services provided by Defendant. Implied in these exchanges was a promise by Defendant to ensure that the sensitive information of Plaintiffs and Class members in their possession was secure.

93. Pursuant to these implied contracts, Defendant obtained Plaintiffs' and Class Members' PII, PHI, and Private Information for Defendant to provide services, for which Defendant is compensated. In exchange, Defendant agreed to, among other things, and Plaintiffs understood that Defendant would: (1) provide services to Plaintiffs and Class members; (2) take reasonable measures to protect the security and confidentiality of Plaintiffs' and Class members' PII, PHI, and Private Information; and (3) protect Plaintiffs' and Class members' PII, PHI, and Private Information in compliance with federal and state laws and regulations and industry standards.

94. Implied in these exchanges was a promise by Defendant to ensure the PII, PHI and Private Information of Plaintiffs and Class members in their possession was only used to provide the agreed-upon reasons, and that Defendant would take adequate measures to protect the sensitive information.

95. A material term of this contract is a covenant by Defendant that it would take reasonable efforts to safeguard that information. Defendant breached this covenant by allowing Plaintiffs' and Class members' PII, PHI, and Private Information to be accessed in the Data Breach.

96. Indeed, implicit in the agreement between Defendant and the patients was the obligation that both parties would maintain information confidentially and securely.

97. These exchanges constituted an agreement and meeting of the minds between the parties: Plaintiffs and Class members would provide their PII, PHI, and Private Information in exchange for services by Defendant. These agreements were made by Plaintiffs and Class members as Defendant's customers.

98. When the parties entered into an agreement, mutual assent occurred. Plaintiffs and Class members would not have disclosed their PII, PHI, and Private Information to Defendant but for the prospect of utilizing Defendant's services. Conversely, Defendant presumably would not have taken Plaintiffs' and Class members' PII, PHI and Private Information if it did not intend to provide Plaintiffs and Class members with their services.

99. Defendant was therefore required to reasonably safeguard and protect the sensitive information of Plaintiffs and Class members from unauthorized disclosure and/or use.

100. Plaintiffs and Class Members accepted Defendant's offer of services and fully performed their obligations under the implied contract with Defendant by providing their PII, PHI, and Private Information directly or indirectly, to Defendant, among other obligations.

101. Plaintiffs and Class Members would not have entrusted their PII, PHI, and Private Information to Defendant in the absence of their implied contracts with Defendant and would have instead retained the opportunity to control their PII, PHI, and Private Information.

102. Defendant breached the implied contracts with Plaintiffs and Class members by failing to reasonably safeguard and protect Plaintiffs' and Class Members' PII, PHI, and Private Information.

103. Defendant's failure to implement adequate measures to protect the PII, PHI, and Private Information of Plaintiffs and Class Members violated the purpose of the agreement between the parties.

104. Instead of spending adequate financial resources to safeguard Plaintiffs' and Class Members' PII, PHI, and Private Information, which Plaintiffs and Class Members were required to provide to Defendant, Defendant instead used that money for other purposes, thereby breaching their implied contracts it had with Plaintiffs and Class members.

105. As a proximate and direct result of Defendant's breaches of their implied contracts with Plaintiffs and Class Members, Plaintiffs and the Class Members suffered damages as described in detail above.

COUNT III
UNJUST ENRICHMENT
(On behalf of Plaintiffs and All Class Members)

106. Plaintiffs incorporate by reference all preceding allegations, as if fully set forth herein.

107. Plaintiffs and Class Members conferred a benefit upon Defendant by using Defendant's services.

108. Defendant appreciated or had knowledge of the benefits conferred upon itself by Plaintiffs. Defendant also benefited from the receipt of Plaintiffs' PII, PHI, and Private Information as this was used for Defendant to administer its services to Plaintiffs and the Class.

109. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiffs' services and their PII, PHI, and Private Information because Defendant failed to adequately protect their sensitive information. Plaintiffs and the proposed Class would not have provided their sensitive information to Defendant or utilized their services had they known Defendant would not adequately protect their PII, PHI, and Private Information.

110. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiffs all unlawful or inequitable proceeds received by it because of their misconduct and Data Breach.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of all others similarly situated, seek judgment against Defendant, as follows:

(a) For an order determining that this action is properly brought as a class action and certifying Plaintiffs as the representatives of the Class and their counsel as Class Counsel;

(b) For an order declaring the Defendant's conduct violates the laws referenced herein;

(c) For an order finding in favor of Plaintiffs and the Class on all counts asserted herein;

(d) For damages in amounts to be determined by the Court and/or jury;

(e) An award of statutory damages or penalties to the extent available;

(f) For pre-judgment interest on all amounts awarded;

(g) For an order of restitution and all other forms of monetary relief; and

(h) Such other and further relief as the Court deems necessary and appropriate.

DEMAND FOR TRIAL BY JURY

Plaintiffs demand a trial by jury of all issues so triable.

Dated: January 10, 2024

Respectfully submitted,

LEVI & KORSINSKY, LLP

By: */s/ Courtney E. Maccarone*
Courtney E. Maccarone (NJ 029842011)
Mark S. Reich*
Gary I. Ishimoto*
LEVI & KORSINSKY, LLP
33 Whitehall Street, 17th Floor
New York, NY 10004
Telephone: (212) 363-7500
Facsimile: (212) 363-7171
Email: cmaccarone@zlk.com
Email: mreich@zlk.com
Email: gishimoto@zlk.com

**pro hac vice* forthcoming

Counsel for Plaintiffs